REMARKS

Claims 11-21 are pending in the present application, claims 1-10 having been cancelled and claims 11-21 having been substituted therefor. Claims 11-20 correspond to original claims 1-10, respectively, and claim 21 is new. The Office Action and cited references have been considered. Favorable reconsideration is respectfully requested.

The examiner has entered an objection to the abstract and the specification. An amended abstract, and a substitute specification are provided herewith. Applicant respectfully submits that no new matter has been entered in the substitute specification. Withdrawal of the objections to the specification and abstract is respectfully requested.

The claims are objected to due a number of informalities noted in the Office Action. Substitute claims have been provided to overcome these objections. Withdrawal thereof is respectfully requested.

Claims 1-10 were rejected under 35 U.S.C. § 112, second paragraph as allegedly failing to comply with the enablement requirement. The Office Action contends that the term "odd order point" is not defined in the specification. Applicant respectfully disagrees. The Examiner's attention is invited to page 15, lines 13-17, which state "let p ∋ $E(F_{2^n})$ be a point of odd order r,..." The Examiner's attention is also

drawn to page 20, lines 28-29, which indicates that in one application of the invention, a public key is the point P of odd order r of the chosen non-supersingular elliptic curve E. Applicant respectfully submits that at least these portions of the specification provide sufficient information regarding the odd order point as to enable one of ordinary skill in the art to make and use the invention. If this rejection is maintained, the Examiner is requested to particularly describe why he believes that this information provided in the specification is insufficient to enable one of ordinary skill in the art to make and use the invention as required under 35 U.S.C. § 112, first paragraph.

Claims 2-3, and 6-8 were rejected under 35 U.S.C. § 112, second paragraph. New claims 2, 12-13 and 16-18 were rewritten with the Examiner's rejections in mind. Applicant respectfully submits that the rewritten claims overcome the objections indicated in the Office Action. Withdrawal of this rejection is thus respectfully requested.

Claims 1-10 were rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. Claim 1 has been amended to recite "a cryptographic method employed between two entities exchanging information via a non-secure communication channel, each of the two entities comprising a memory readable by a machine, tangibly embodying

a program of instructions executable by the machine to perform the method, the method including the step of multiplying an odd order point of a non-supersingular elliptic curve by an integer, ...". Applicant respectfully submits that as amended, claim 1 properly complies with 35 U.S.C. § 101 and present statutory subject matter. Applicant respectfully requests reconsideration and withdrawal of this rejection.

Claims 6 and 8 were rejected under 35 U.S.C. § 101 as being improper process claims. Applicant's new claims 16 and 18, corresponding to original claims 6 and 8 are drafted so as to overcome this rejection. Withdrawal thereof is respectfully requested.

Claim 1 was rejected under 35 U.S.C. § 103 as being unpatentable over "Fast Key Exchange with Elliptic Curve Systems" by Schroeppel et al. (Schroeppel), "A Public Key Cryptosystem Based on Elliptic Curves over Z/nZ Equivalent to Factoring" by Meyer et al. (Meyer), "Elliptic Curve Cryptosystems and Their Applications" by Koyama et al. (Koyama) and U.S. Patent 6,141,420 to Vanstone et al. (Vanstone). Claim 8 was rejected under 35 U.S.C. § 103 as being unpatentable over Schroeppel, Meyer, Koyama and Vanstone as applied to claim 1, in further view of "An Elliptical Curve Implementation of the Finite Field Digital Signature Algorithm" by Koblitz. These rejections are respectfully

traversed for the following reasons. Reference is made to new claims 11 and 18.

The invention relates to a cryptographic method employed between two entities exchanging information over a non-secure communication channel, for example a cable or radio network. The method according to the invention assures the confidentiality and the integrity of information transfer between the two entities. In this respect, it concerns an improvement to cryptosystems employing calculations on an elliptic curve, and reduces calculation time.

Precisely, a step of multiplying an odd order point of a non-supersingular elliptic curve in a cryptographic method is performed by addition and halving operation of points of the elliptical curve. The halving application is beneficial for scalar multiplication of a point on an elliptic curve. In fact, if affine coordinates are used, it is possible to replace all doublings of a point of a scalar multiplication by halving of a point (see also the specification page 4, line 26 to page 5, line 10).

Reviewing the Office Action, the Examiner appears to consider that the step of multiplying further includes addition and halving operations of the points of the elliptic curve. In this respect, the Office Action cites Schroeppel and Koyama to allege the obvious use of multiplying,

doubling/addition and halving operations in a cryptographic method in an elliptic curve domain. However, Applicant respectfully submits that none of these patents recite that the step of multiplying in the cryptographic method is performed by addition and halving of points of the elliptic curve as is recited in claim 11. For at least this reason, Applicant respectfully submits that claim 11 is patentable over the prior art of record whether taken alone or in combination as asserted in the Office Action. Claim 18 depends from and includes the recitations of claim 11. Applicant respectfully submits that claim 8 is patentable over the prior art of record for at least the reasons discussed above with respect to claim 11.

Applicant notes with appreciation the indication that original claims 2-7 and 9-10 (corresponding to new claims 12-17 and 19-20) are patentable over the prior art of record in view of the lack of prior art rejections of these claims.

In view of the above amendments and remarks, Applicant respectfully requests reconsideration and withdrawal of the outstanding rejections of record. Applicant submits that the application is in condition for allowance and early notice to this effect is most earnestly solicited.

If the Examiner has any questions he is invited to contact the undersigned at 202-628-5197.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant

By 
Ronni S. Jillions
Registration No. 31,979

RSJ:tbs
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
G:\BN\B\Bonn\Knudsen2\2005Jun13 AMD.doc

Attachments: Annotated Specification Sheet Showing Changes;
Replacement Specification Sheet